Silicon Valley Software Lawyer Kristie Prinz to Present Upcoming Webinar on "Drafting Software Hosting Agreements"

Silicon Valley Software Lawyer Kristie Prinz will be presenting an upcoming webinar with FieldFisher partner Laura Berton on "Drafting Software Hosting Agreements: Service Availability, Performance, Data Security, Other Key Provisions" for Strafford on Thursday, July 25th from 10 a.m. to 11:30 a.m. PST. For more information on the program, please **click here**.

Software Industry Concerned About the Potential Impact of AB-5 on Gig Economy

The Software Industry is closely following legislation in California that, if passed, could have a huge impact on Gig workers and the software companies that rely on them.

The legislation at issue is AB 5, which would codify and expand the California Supreme Court's recent decision in **Dynamex Operations v. Superior Court** (2018) 4 Cal. 5th 903. The text of the proposed legislation is available **here**.

According to **The Intercept**, the bill was sponsored by Lorena Gonzalez, a Democratic assemblywoman from San Diego. **The Intercept** reports that that California is losing an estimated $7 billion in payroll tax annually due to the misclassification of employees as independent contractors, so the state is eager to close the loophole.

Obviously, Uber and Lyft, directly oppose the legislation, since it would directly impact their current Gig worker business model. In fact, **The Los Angeles Times** has reported that Uber and Lyft have actually paid drivers to organize protests against the legislation.

For Uber and Lyft, the obvious concern is that the passage of AB-5 in California could prompt other states to pass their own versions of the legislation, or even, that similar legislation could be passed at the federal level, which could potentially expand the impact of the legislation far beyond the borders of California.

Both **The Intercept** and **The Los Angeles Times** are reporting that Uber and Lyft have each warned investors of this potential risk in recent regulatory filings. Indeed, an investment publication, **Investorplace**, warns that the passage of the bill will have a very detrimental impact on both companies.

The bottom line is that software companies who have built business models around the Gig worker model may soon be forced to either cease operations in California or, alternatively, to change their models for the state, if AB-5 is passed and signed into law, so if your company has been developed around this model or you are building a company relying on this model, you will want to follow this legislation closely as it moves through the California legislature.

News Update on FTC's Application of Safeguards Rule to Software Company

News Update 7.17.19

Facebook Agrees to Record $5 Billion Settlement with FTC on Privacy Practices

Multiple media outlets are reporting today that the Federal Trade Commission has agreed to settle its case against Facebook on its privacy practices for $5 Billion.

The Wall Street Journal reports that the vote by FTC commissioners was 3-2 in favor of accepting the agreement and split along party lines with the Republican majority favoring the settlement. According to **The Wall Street Journal**, the matter next goes the the Justice Department's civil division for final review.

According to the **Mercury News**, assuming reports are correct, this will be the largest fine imposed to date by the U.S. government on a tech company. **The Washington Post** reports that the fine is more than 200 times higher than any previous fine.

Interestingly enough, **The Wall Street Journal** is reporting that the fine obtained by the FTC exceeds what the European Union could have obtained under its privacy laws.

The Washington Post predicts that the settlement will impose serious consequences on Facebook that go far beyond just a $5 billion fine. However, **The Washington Post** acknowledges that the dissenting commissioners opposed the settlement because they wanted some assessment of personal liability against CEO Mark Zuckenberg; commissioners reportedly decided to accept a settlement without any such assessment in order to ensure that the matter did not end up in litigation.

While controversial, the FTC's enforcement action in this matter still sets a significant precedent for the software industry with respect to the consequences of not protecting data uploaded to or generated by software. Software companies are on notice: the FTC is closely following your privacy practices and may assess fines in the billions of dollars against you if you fail to take sufficient steps to protect user data.

Should Law Enforcement Agencies' Use of Facial Recognition Software Be Subject to Regulation?

As **The New York Times** and **The Washington Post** recently reported, facial recognition software is being heavily utilized by government agencies, who are using the software to search state driver's license databases, despite the fact that

most of the photos in the databases are of citizens who have never committed a crime and have never given any sort of consent to the searches. The reports have raised concerns about the lack of regulation and oversight currently with respect to the use of facial recognition software by law enforcement.

According to a report by **The New York Times**, since 2011, the FBI has run nearly 400,000 facial recognition searches of federal and local databases, including DMV records. **The Washington Post** reports that the FBI is currently running about 4000 searches per month.

Moreover, **The New York Times** and **The Washington Post** are reporting that in states offering driver licenses to undocumented immigrants, Immigration and Customs Enforcement ("ICE") is using the software to conduct searches on undocumented immigrants.

The Washington Post reports that twenty-one (21) states and the District of Columbia allow federal investigators to scan driver's license photos, and that those searches generally require no more than an email request to conduct the search.

A number of lawmakers in Washington are raising concerns about the recent revelations, and two cities, San Francisco and Somerville, MA, have now imposed a ban preventing police and public agencies from using the software. **The Washington Post** reports that a privacy coalition has petitioned the Homeland Security Committee for the Department of Homeland Security ("DHS") to stop using the technology.

What are the arguments being raised in favor of greater regulation of law enforcement's use of the technology?

First and foremost, proponents for greater regulation argue that running facial recognition searches against photos of law-abiding citizens is a huge privacy violation. Secondly, they argue the scope of it use by law enforcement is too

broad, since it has been used not only for the identification of criminal suspects but also to find witnesses, victims, and bystanders. Third, they argue its use often constitutes a breach of trust, since states encourage undocumented immigrants to submit their information to the databases and then proceed to to tun it over to ICE. Fourth, they argue that use of the software heightens the risk of misidentification and false arrest due to inaccuracies with how certain facial features are detected.

All in all, it is clear that law enforcement considers facial recognition software to be a valuable investigative tool. However, there are clearly some valid concerns with how the software is being used that warrant further consideration. Should law enforcement really be able to conduct these types of searches without a warrant? Should ICE be able to conduct searches of undocumented immigrants who have been encouraged to submit information for inclusion in a database? What kind of checks should be in place on law enforcement's use of software that that has inherent inaccuracies?

Silicon Valley SaaS Lawyer Kristie Prinz to Speak at Upcoming Webinar on SaaS Agreements

Clear Law Press Release 7.5.19

Silicon Valley Software Lawyer Kristie Prinz to Speak at Upcoming Webinar on Software Hosting Agreements

Strafford Press Release 7.5.19

FTC Sends Warning to IoT Companies on the Importance of Secure Software Development with Enforcement Action Against D-Link

Internet of Things ("IoT") companies are on notice: the FTC is concerned about the the security of software installed to IoT and smart home products and is prepared to take enforcement action against companies to ensure that consumers are protected.

The FTC has just announced the proposed settlement of its case against D-Link filed in January, 2017, which mandates that D-Link put in place and maintain a comprehensive software security program for the next 20 years that incorporates

certain specified requirements, including a “secure software development process” that incorporates specified software development safeguards to ensure the security of its devices.

These FTC imposed requirements include the following:

- Specifying in writing how functionality and features secure the devices;
- Engaging in threat modeling to identify potential security risks;
- Reviewing every planned release of code with automated static analysis tools;
- Performing pre-release vulnerability testing on each planned release of code;
- Performing ongoing code maintenance to address vulnerabilities as they are identified;
- Adopting remediation processes to address identified security flaws at any stage of the development process;
- Monitoring research on possible vulnerabilities to devices;
- Setting up a process for receiving and validating vulnerability reports from security researchers;
- Making automatic firmware updates to devices;
- Notifying customers at least 60 days in advance of any decision to stop making security updates to a devices; and
- Providing biennial security training for personnel and any vendors involved with the device software.

In addition to imposing the above requirements on D-LInk, the order gives the FTC the power of oversight to ensure ongoing compliance, and requires D-Link to obtain routine third party assessments by a professional with credentials specified by the FTC to perform in-depth reviews of D-Link’s security practices. The FTC specifically mandates that the assessment meet an approved standard as defined by the FTC: the International Electrotechnical Commission (“IEC”) standard for the secure product development life cycle. The FTC

announcement is attached **here** and its order is **attached here.**

What prompted the FTC case against D-Link? The FTC complaint filed against D-Link alleged a failure by D-Link to take "reasonable" steps to secure software constituting "unfair acts or practices in or affecting commerce, in violation of Section 5 of the FTC Act, 15 U.S.C. Sections 45(a) and 45 (n)" and misrepresentations regarding D-Link's security practices constituting a "defective act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S. C. Section 45(a)." The FTC Complaint against D-Link is attached **here**.

What do companies engaged in IoT software development need to take away from this enforcement action? First of all, companies need to be aware that the FTC is applying its regulatory powers against companies to ensure that they are securing software in accordance with any representations made to consumers. Second of all, companies need to be aware that the FTC is looking to certain published standards by the IEC to provide the industry standards for software in this space, so IEC compliance certification may provide the measure of a company's compliance with its security obligations. Third, the FTC has provided some suggested guidelines for companies to follow in the following publications: **Careful Connections: Building Security in the Internet of Things** and **Start With Security: Lessons Learned from FTC Cases.**

FTC Puts Software Companies and Service Providers on

Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule

The Federal Trade Commission ("FTC") has put software companies and software service providers on notice it intends to interpret the Gramm-Leach-Bliley Act's Safeguards Rule broadly to apply to businesses which make available software or services that serve financial, payroll, and accounting purposes and collect sensitive data on consumers and their employees.

The FTC recently announced its settlement of a complaint filed against LightYear Dealer Technologies, LLC which does business as Dealerbuilt, which required Dealerbuilt as condition of the settlement to develop, implement and maintain an information security program that incorporates the minimum requirements specified by the FTC and submit to third party compliance assessments and annual certifications over a period of the next 20 years.

The FTC's specified minimum requirements for Dealerbuilt's information security program included the following:

- Develop, implement, maintain and record in writing an Information Security Program;
- Make available the written program, evaluations of the program, and updates on the program, to the company's board of directors or governing body, or if none exists, the senior officer responsible for the program at least once per annual period and after any data breach;
- Identify an employee or employees responsible for the coordination of the program;
- Provide written assessment annually and after any data breach of any potential data breach risks;

- Develop written safeguards to ensure data security including the following:
    - Training of all employees at least once every annual period on how to protect personal information;
    - Technical measures monitoring networks, systems to identify attempted data breaches;
    - Access controls on databases containing personal information, which (a) restrict the ability to connect to only approved IP addresses; (b) require authentication to access the databases; and (c) limit the access of employees to only those databases as necessary to perform their duties;
    - Encrypt all social security numbers and financial account information;
    - Implement policies and procedures for secure installation and inventory on an annual basis
- Perform assessment annually and after any data breach of the sufficiency of safeguards and modify the program as necessary;
- Conduct test annually and after any data breach of effectiveness of safeguards, which shall include vulnerability testing every four months and after a data breach, and annual penetration testing, as well as after any data breach;
- Ensuring that contracts with any service providers ensure compliance with safeguards; and
- Evaluate and make adjustments to program upon any changes to operations or business or in event of any data breach. or on an annual basis.

The FTC Order also mandates that an information security assessment be conducted initially and biennially by a third party professional approved by the Associate Director for Enforcement for the Bureau of Consumer Protection at the FTC, and that the assessor will be required to provide the documents relevant to the assessment to the FTC for review

within 10 days following the completion of the initial review and then on demand. Furthermore, the Order requires the senior corporate manager or senior officer of Dealerbuilt to submit annual written certifications to the FTC, and that within a reasonable time following any discovery of a data breach, or at least 10 days following the provision of first notice of any data breach, Dealerbuilt must send a report to the FTC of any data breach, which meets certain specified requirements. Also, the Order permanently enjoins all individuals affiliated with Dealerbuilt from violating any provisions of the Safeguards Rule, and makes the Order applicable to all businesses connected to Dealerbuilt, which Dealerbuilt is to be broadly interpreted and Dealerbuilt is required to identify in detail via compliance reports, accompanied by sworn affidavits.

The FTC also imposes broad recordkeeping requirements on Dealerbuilt through the Order, requiring Dealerbuilt to create and retain for the next 20 years accounting records of all revenues collected, personnel records, consumer complaint records and responses to those records, and any documents relied upon to prepare mandate assessments and to demonstrate full compliance with the order.

Finally, within 10 days of any request by the FTC, Dealerbuilt is required to furnish compliance reports to the FTC or other requested information accompanied by sworn affidavits.

The FTC announcement is attached **here** and the Order attached **here**.

What prompted this broad enforcement action by the FTC against DealerBuilt? According to the **FTC Complaint**, a series of security failures resulted in the breach of a backup database through a storage device beginning in late October 2016, which resulted in the breach of personal information of nearly Seventy Thousand consumers, which included full names and addresses, telephone numbers, social security numbers, drivers

license numbers, and birthdates of consumers as well as wage and financial account information of dealership employees. The **FTC Complaint** further alleges that Dealerbuilt failed to detect the breach and only learned of it after a customer called its chief technology officer demanding to know why customer data was publicly available on the Internet.

The **FTC Complaint** alleged that Dealerbuilt was a financial institution as defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6809(3)(A) as a result of being "significantly engaged in data processing for its customers, auto dealerships that extend credit to customers." **The Complaint** alleged that the "failure to employ measures to protect personal information" constituted an "unfair act or practice" and that the failures to (a) "develop, implement, and maintain a written information security program"; (b) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information" and "assess the sufficiency of any safeguards in place to control those risks"; and (c) to design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards" constituted a violation of the Safeguards Rule and an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

What should software companies and service providers take away from this FTC enforcement action? First and foremost, the FTC is making a definitive statement that if you are in the business of providing software or software services that have any sort of financial or accounting function to them, you are a financial institution for purposes of Gramm-Leach-Bliley and the Safeguards Rule is going to be deemed to apply to your business. Second, the FTC considers service providers accountable for the protection of any personal data they collect or store. Third, the FTC expects businesses using third party software or providers to have contracts in place

with those software companies or service providers imposing security requirements, monitoring requirements, and explicitly requiring them to follow websites reporting on known vulnerabilities. Fourth, the FTC expects businesses to train and supervise employees on how to ensure the security of the company. The FTC specifically points businesses in its announcement to comply with its publication, **Start with Security: Lessons Learned from FTC Cases**.FTC Puts Software Companies and Service Providers on Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule